Rate-Distortion-Based Physical Layer Secrecy in Multimode Fiber

Eva C. Song, Emina Soljanin, *Senior Member, IEEE*, Paul Cuff, *Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

Abstract

Optical networks are vulnerable to physical layer attacks; wiretappers can improperly receive messages intended for legitimate recipients. Our work considers an aspect of this security problem within the domain of multimode fiber (MMF) transmission. MMF transmission can be modeled via a broadcast channel in which both the legitimate receiver's and wiretapper's channels are multiple-input-multiple-output complex Gaussian channels. Source-channel coding analyses based on the use of distortion as the metric for secrecy are developed. Alice has a source sequence to be encoded and transmitted over this broadcast channel so that the legitimate user Bob can reliably decode while forcing the distortion of wiretapper, or eavesdropper, Eve's estimate as high as possible. Tradeoffs between transmission rate and distortion under two extreme scenarios are examined: the best case where Eve has only her channel output and the worst case where she also knows the past realization of the source. It is shown that under the best case, an operationally separate source-channel coding scheme guarantees maximum distortion at the same rate as needed for reliable transmission. Theoretical bounds are given, and particularized for MMF. Numerical results showing the rate distortion tradeoff are presented and compared with corresponding results for the perfect secrecy case.

E. C. Song, P. Cuff and H. V. Poor are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA e-mail: ({csong,cuff, poor}@princeton.edu).

E. Soljanin is with Bell Labs, Alcatel-Lucent, Murray Hill, NJ 07974, USA e-mail(emina@alcatel-lucent.com)

Index Terms

rate-distortion, MIMO, optical fiber communication, source-channel coding, secrecy

I. INTRODUCTION

Single mode fiber systems are believed to have reached their capacity limits. In particular, techniques such as wavelength-division multiplexing (WDM) and polarization-division multiplexing (PDM) have been heavily studied in the past few years, leaving little room for further improvement in capacity [1]. Space-division multiplexing (SDM) is a promising solution for meeting the growing capacity demands of optical communication networks. One way of realizing SDM is via the use of multimode fiber (MMF). While multimode transmission provide greater capacity, the security of such systems can be an issue because an wiretapper can eavesdrop upon MMF communication by simply bending [2] the fiber. MMF is a multiple-input-multiple-output (MIMO) system [1] that captures the charateristics of crosstalk among different modes. The secrecy capacity of a Gaussian MIMO broadcast channel was studied by [3], but the result cannot be applied directly to MMF because the channel is not the same. The secrecy capacity of this channel was studied in [2] where it is shown that the channel conditions required for perfect secrecy are quite demanding.

Equivocation is commonly used to quantify secrecy in the study of physical layer security of communication systems. However, while equivocation is a reasonable metric for perfect secrecy, its interpretation for partial secrecy is less clear. Distortion is an alternative measure of secrecy that provides an intuitive measure of partial secrecy by comparing the difference between the information intended for the legitimate receiver and eavesdropper's estimate of it. Distortion was used in [4] and [5] as a metric for secrecy in the context of a noiseless network with secret key sharing. In this work, we are concerned with physical layer secrecy in MMF systems. In order to examine trade-offs associated with such secrecy, we will consider partial secrecy and thus will use a distortion-based formulation. This prompts us to formulate this problem as a

source-channel coding problem. Along the lines studied in a general setting in [6], some results of which can be directly applied to MMF systems.

The rest of the paper is structured as follows. In Section II, we introduce the system model and define the source-channel coding problem under two scenarios. In Section III, we provide theoretical bounds with source-channel coding for general broadcast channel when the channels are fixed. In Section IV, we apply the general results to the MMF model under the two scenarios. In Section V, we provide numerical evaluation to the MMF source-channel model under Hamming distortion. In Section VI, we discuss the generalization of this model to the case of random channels in which the channel state information (CSI) is not available to the transmitter. Finally, in Section VII, we conclude the paper and discuss open problems from this work.

II. System Model

A source node (Alice) has an independent and identically distributed (i.i.d.) sequence S^k that she intends to transmit over an MMF such that a legitimate user (Bob) can reliably decode the source sequence, while keeping the distortion between an eavesdropper (Eve) and Alice as high as possible. An M-mode MMF is modeled as a memoryless MIMO channel with input X, which is an M-dimensional complex vector. Unlike wireless MIMO which has a total power constraint, MMF channels have the following per mode power constraint averaged over n uses of the channel:

$$\frac{1}{n}\sum_{i=1}^{n}|X_i^{(m)}|^2 \leq 1 \quad \text{for all modes } m \in [1:M]. \tag{1}$$

More generally (as in [3]), we will consider a power constraint of the form

$$\frac{1}{n}\sum_{i=1}^{n}X_iX_i^{\dagger} \preceq Q, \tag{2}$$

where $Q \in \{A \in \mathcal{H}^{M\times M} : A \succeq 0, A_{ii} = 1\}$ and $\mathcal{H}$ denotes the set of Hermitian matrices. One element in this set is the identity matrix I (constraint (1)). We will focus on $Q = I$, and later in

Section VI we will explain why this is the case of our particular interest. A detailed discussion of the MMF channel model can be found in [1]. This is a joint source-channel coding problem. The source sequence S^k is mapped to the channel input sequence X^n through a source-channel encoder.

A. The Legitimate User Communications Model

The channel between Alice and Bob is complex, Gaussian, MIMO, with input $X \in \mathbb{C}^M$ as described above, and output $Y \in \mathbb{C}^M$ given by

$$Y \;=\; HX + N, \tag{3}$$

where $N \sim \mathcal{CN}(0, \sigma_N^2 I, 0)$ is M-dimensional, uncorrelated, zero-mean, complex, Gaussian noise and H is an $M \times M$ complex matrix. Bob's channel matrix H is of the form

$$H \;=\; \sqrt{E_0 L}\Psi, \tag{4}$$

where $\Psi \in \mathbb{C}^{M\times M}$ is unitary and $E_0 L$ is a constant scalar that measures the average power of the channel. We refer to $E_0 L/\sigma_N^2$ as the SNR of the channel.

Matrix Ψ, the unitary factor of the channel H, describes the modal crosstalk [1]. Ψ is uniformly distributed among all unitary matrices in $\mathbb{C}^{M\times M}$, but Ψ stays constant during n channel uses. The CSI (the actual realization of Ψ) is known only to the receiver but is unknown to the transmitter due to the long round-trip delay over large distances common in optical transmission.

Upon receiving Y^n, Bob makes an estimate $\hat{S}^k$ of the original source sequence S^k. For almost lossless reconstruction, we require the probability that Bob's reconstruction differs from the original goes to zero asymptoticly with the source blocklength. That is,

$$\mathbb{P}[S^k \neq \hat{S}^k] \to_k 0.$$

B. The Eavesdropper Communications Model

The channel between Alice and Eve is also complex, Gaussian, MIMO, with input $X \in \mathbb{C}^M$ as described above, and output $Z \in \mathbb{C}^M$ given by

$$Z \;=\; H^e X + N^e, \tag{5}$$

where $N^e \sim \mathcal{CN}(0, \sigma^2_{N^e} I, 0)$ is M-dimensional uncorrelated, zero-mean, complex, Gaussian noise, and H^e is an $M \times M$ complex matrix. Eve's channel matrix H^e is of the form

$$H^e \;=\; \sqrt{E_0 L^e}\sqrt{\Phi}\Psi^e, \tag{6}$$

where $\Psi^e \in \mathbb{C}^{M\times M}$ is unitary, Φ is diagonal with positive entries, and $E_0 L^e$ is the average power of Eve's channel.

Note that Eve has a different signal to noise ratio $\text{SNR}^e = E_0 L^e / \sigma^2_{N^e}$. The channel matrix has a unitary component Ψ^e which is statistically the same as Ψ. The diagonal component of Φ corresponds to the mode-dependent loss (MDL) as introduced in [1]. The diagonal matrix Φ is also random, and its distribution will be discussed later in Section VI. It is assumed that Ψ, Ψ^e and Φ are constant throughout the block and the eavesdropper has the CSI. We will examine two extreme cases based on the amount of side information Eve has.

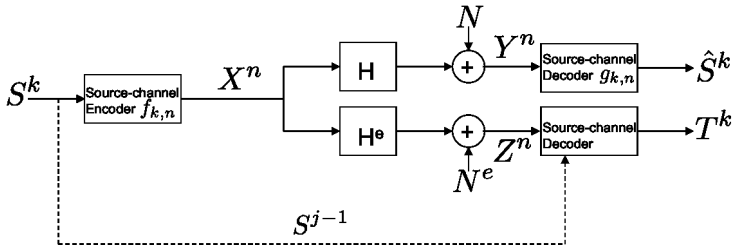

Fig. 1: MMF source-channel coding model. The physical channel is a MIMO broadcast channel.

1) No causal information available to Eve: The case in which Eve has only her own channel output but no side information about the source corresponds to the best scenario for the legitimate

users of the network, Alice and Bob. With the channel output alone, Eve has very limited resources in hand to make the estimate. This model is defined mathematically as follows. We use italic capital letter to denote the support of a random variable (e.g. $\mathcal{X}$ denotes the support of X) . Let $f_{k,n} : \mathcal{S}^k \mapsto \mathcal{X}^n$ be a source-channel encoder and $g_{k,n} : \mathcal{Y}^n \mapsto \mathcal{S}^k$ be the corresponding decoder. Let t^k be Eve's estimation of original source sequence s^k. For a distortion measure $d : \mathcal{S} \times \mathcal{T} \mapsto R^+$, the distortion between two sequences is defined to be the per-letter average distortion $d^k(s^k, t^k) = \frac{1}{k}\sum_{i=1}^{k} d(s_i, t_i)$. The system model is shown in Fig. 1; however, the dashed line represents additional information that is not available to the eavesdropper in this first scenario. We use the lower case $t^k(z^n)$ to denote Eve's deterministic estimation functions of her observation z^n and the capital letter $T^k = t^k(Z^n)$ to denote the function of the random variable Z^n. The following definitions in this section are for constant fixed channels.

Definition 1. *For a given distortion function $d(s, t)$, a rate distortion pair (R, D) is achievable if there exists a sequence of encoder/decoder pairs $f_{k,n}$ and $g_{k,n}$ such that*

$$\frac{k}{n} = R,$$

$$\lim_{n\to\infty} \mathbb{P}[S^k \neq \hat{S}^k] = 0,$$

and

$$\liminf_{n\to\infty} \min_{t^k(z^n)} \mathbb{E}[d(S^k, t^k(Z^n))] \geq D.$$

Note that the rate-distortion pair (R, D) captures the tradeoff between Bob's rate for reliable transmission and Eve's distortion, which is different from rate-distortion theory in the traditional sense.

2) With causal information available to Eve: On the other hand, we are also interested in the case in which, at each time instance j, Eve gets to see the past realization of the source sequence S^{j-1}. This would be the worst scenario for the legitimate users. The definition for an

achievable rate distortion pairs (R, D) is similar to Definition 1 given in the previous subsection except the last condition is replaced by

$$\liminf_{n\to\infty} \min_{\{t_j(z^n,s^{j-1})\}_{j=1}^k} \mathbb{E}\left[\frac{1}{k}\sum_{j=1}^{k} d(S_j, t_j(Z^n, S^{j-1})\right] \geq D.$$

The system model is shown in Fig. 1 with dashed line representing the availability of the causal information. The maximum distortion Δ is defined as

$$\Delta \triangleq \min_t \mathbb{E}[d(S,t)]. \tag{7}$$

In the next section we apply results from [6] and [7] to our source-channel setting for a general broadcast channel. However, the results in [7] were not derived in the context of a noisy communication channel. Extending [7] for the noisy channel case of interest in this work turns out to require a so-called "strong secrecy" channel coding proof. This is presented in Section III. In the following sections, we apply the theoretical results to the MMF channels by choosing proper auxilliary random variables. Finally we will discuss how this can be generalized to random channels when no CSI is available at the transmitter.

III. Theoretical Bounds

In this section, instead of focusing on MMF, we consider a more general problem in which the channel is any noisy memoryless broadcast channel. Let $P_{YZ|X}$ denote the transition probability of the broadcast channel in each use. We first make some general observations on the communication between Alice and Bob, as well as the communication between Alice and Eve. If Eve is not present, Alice and Bob can communicate losslessly at any rate lower than $R_0 \triangleq \frac{\max_X I(X;Y)}{H(S)}$ because separate source-channel coding is optimal for point-to-point communication. Ideally, we want to force maximum distortion Δ upon Eve (the average distortion achieved by guesses based only on the prior distribution of the source). But higher distortion to Eve may come at the price of a lower communication rate to Bob. The content of this section is organized as follows: the rate-distortion region for the "no causal information" case is first given in Theorem 1; to prepare

for the achievability proof of Theorem 1, an operational separation scheme is discussed; finally, an achievable rate-distortion region is given in Theorem 5 for the causal case under Hamming distortion.

We now state the rate-distortion result for general source-channel coding with an i.i.d. source sequence and a discrete memoryless broadcast channel $P_{YZ|X}$ when **no causal information** is available to Eve. In the following theorem, we will see that the source sequence can be delivered almost losslessly to Bob at a rate arbitarily close to R_0 while the distortion to Eve is kept at Δ, as long as the secrecy capacity is positive. We use the symbol –□– to denote a Markov relation.

Theorem 1. *For an i.i.d. source sequence S^k and memoryless broadcast channel $P_{YZ|X}$, if there exists W–□–X–□–YZ such that $I(W;Y) - I(W;Z) > 0$, then (R, D) is achievable if and only if*

$$R < \frac{\max_X I(X;Y)}{H(S)}, \tag{8}$$

$$D \leq \Delta \tag{9}$$

Remark: The requirement $R_s = I(W;Y) - I(W;Z) > 0$ implies the existence of a secure channel with a positive rate, i.e. the eavesdropper's channel is not less noisy than the intended receiver's channel. So instead of demanding a high secure transmission rate R_s as in perfect secrecy defined under equivocation $H(S^k|Z^n) \approx H(S^k)$, we only need to ensure the existence of a secure channel regardless of the actual rate R_s as long as it is strictly positive.

The converse is straightforward. Each of the inequalities (8) and (9) is true individually for any channel and source, (8) by channel capacity coupled by optimality of source-channel separation, and (9) by definition.

This paper proposes a source-channel coding scheme that can achieve the rate and distortion in Theorem 1. The scheme is based on recent work in [6]. The idea for achievability is to

operationally separate the source and channel coding (see Fig. 2). The source encoder compresses the source and splits the resulting message into a private message and a non-private message. A channel encoder is cancatenated digitally with the source encoder so that the channel delivers both the private and non-private messages reliably to Bob and keeps the private message secret from Eve, as in [8]. The overall source-channel coding rate will have the following form: $R = \frac{k}{n} = \frac{k}{\log|\mathcal{M}|} \cdot \frac{\log|\mathcal{M}|}{n} = \frac{R_{ch}}{R_{src}}$, where $|\mathcal{M}|$ is the total cardinality of the private and the non-private messages; R_{ch} and R_{src} are the channel coding and source coding rates, respectively.

Let us look at two models in the following subsections that will help us establish the platform for showing the achievability of Theorem 1.

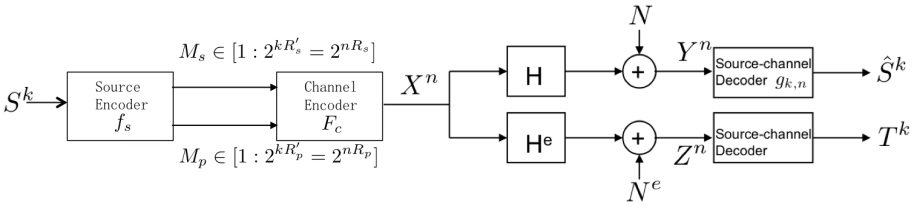

Fig. 2: Operational Separate Source-Channel Coding

A. Channel Coding and Strong Secrecy

Consider a memoryless broadcast channel $P_{YZ|X}$ and a communication system with a private message M_s and a non-private message M_p that must allow the intended receiver to decode both M_s and M_p while keeping the eavesdropper from learning anything about M_s. Problems like this were first studied by Csiszár and Körner [8] in 1978, as an extension of Wyner's work in [9]. Their model differs from ours in that, the second receiver (the eavesdropper in our case) is required to decode the public message M_p. The mathematical formulation and result of our channel model is stated below. We focus on the message pairs (M_s, M_p) whose distribution satisfies the following

$$P_{M_s|M_p=m_p}(m_s) \;=\; 2^{-nR_s} \tag{10}$$

for all (m_s, m_p). Later we will show a source encoder can always prepare the input messages to the channel of this form.

Definition 2. *A (R_s, R_p, n) channel code consists of a channel encoder F_c (possibly stochastic) and a channel decoder g_c such that*

$$F_c : \mathcal{M}_s \times \mathcal{M}_p \mapsto \mathcal{X}^n$$

and

$$g_c : \mathcal{Y}^n \mapsto \mathcal{M}_s \times \mathcal{M}_p$$

where $|\mathcal{M}_s| = 2^{nR_s}$ and $|\mathcal{M}_p| = 2^{nR_p}$.

Definition 3. *The rate pair (R_s, R_p) is achievable under weak secrecy if for all (M_s, M_p) satisfying (10), there exists a sequence of (R_s, R_p, n) channel codes such that*

$$\lim_{n\to\infty} \mathbb{P}[(M_s, M_p) \neq (\hat{M}_s, \hat{M}_p)] = 0$$

and

$$\lim_{n\to\infty} \frac{1}{n} I(M_s; Z^n | M_p) = 0.$$

Note that because the eavesdropper may completely or partially decode M_p, the secrecy requirement is modified accordingly to consider $I(M_s; Z^n|M_p)$ instead of $I(M_s; Z^n)$.

Theorem 2 (Theorem 3 in [6])**.** *A rate pair (R_s, R_p) is achievable under weak secrecy if*

$$R_s \leq I(W;Y|V) - I(W;Z|V), \tag{11}$$

$$R_p \leq I(V;Y) \tag{12}$$

for some V–□–W–□–X–□–YZ.

The proof can be found in [6]. Let us denote the above region as $\mathcal{R}$. We now strengthen the result by considering strong secrecy introduced in [10]. Later we will use strong secrecy to connect the operationally separate source and channel encoders.

Definition 4. *The rate pair* (R_s, R_p) *is achievable under strong secrecy if for all* (M_s, M_p) *satisfying* (10)*, there exists a sequence of* (R_s, R_p, n) *channel codes such that*

$$\lim_{n\to\infty} \mathbb{P}[(M_p, M_s) \neq (\hat{M}_s, \hat{M}_p)] = 0$$

and

$$\lim_{n\to\infty} I(M_s; Z^n|M_p) = 0$$

Theorem 3. *A rate pair* (R_s, R_p) *achievable under weak secrecy is also achievable under strong secrecy.*

For simplicity, we consider only the case in which $|\mathcal{Z}|$ is finite in the following. Generalization to $\mathcal{Z} = \mathbb{R}$ can be done by considering Z_Δ, a quantized version of Z, as in [11]. The following two lemmas will assist the proof of Theorem 3 by providing a sufficient condition for satisfying the secrecy constraint $\lim_{n\to\infty} I(M_s; Z^n|M_P) = 0$.

Lemma 1. *If* $||P_{Z^n|M_p=m_p}P_{M_s|M_p=m_p} - P_{Z^nM_s|M_p=m_p}||_{TV} \leq \epsilon \leq \frac{1}{2}$*, then*

$$I(M_s; Z^n|M_p = m_p) \leq -\epsilon \log \frac{\epsilon}{|\mathcal{M}_s||\mathcal{Z}^n|}.$$

This lemma was also discussed in [12] and its proof can be found in [13].

Lemma 2. *If for every* (m_s, m_p)*, there exists a measure* θ_{m_p} *on* $\mathcal{Z}^n$ *such that*

$$||P_{Z^n|M_p=m_p,M_s=m_s} - \theta_{m_p}||_{TV} \leq \epsilon_n$$

then

$$\lim_{n\to\infty} I(M_s; Z^n|M_p) = 0$$

where $\epsilon_n = 2^{-n\beta}$ *for some* $\beta > 0$*.*

A proof of Lemma 2 is given in Appendix A.

If there exist channel codes such that $\mathbb{P}[(M_s, M_p) \neq (\hat{M}_s, \hat{M}_p)] \to_n 0$ and measure θ_{m_p} for all m_p such that $||P_{Z^n|M_p=m_p,M_s=m_s} - \theta_{m_p}||_{TV} \leq \epsilon_n$, then Theorem 3 follows immediately. The existence of such a code and measure is assured by the same codebook construction and choice of measure as in [12].

B. Source Coding

Recall from our problem setup in Section II that the sender Alice has an i.i.d. source sequence S^k. A source encoder is needed to prepare S^k by encoding it into a pair of messages (M_s, M_p) that satisfies $P_{M_s|M_p=m_p}(m_s) = 2^{-kR'_s} = 2^{-nR_s}$ so that it forms a legitmate input to the channel model in Section III-A.

Definition 5. *An (R'_s, R'_p, k) source code consists of an encoder f_s and a decoder g_s such that*

$$f_s : \mathcal{S}^k \mapsto \mathcal{M}_s \times \mathcal{M}_p$$

$$g_s : \mathcal{M}_s \times \mathcal{M}_p \mapsto \mathcal{S}^k$$

where $|\mathcal{M}_s| = 2^{kR'_s}$ and $|\mathcal{M}_p| = 2^{kR'_p}$.

Definition 6. *A rate distortion triple (R'_s, R'_p, D) is achievable under a given distortion measure $d(s,t)$ if there exists a sequence of (R'_s, R'_p, k) source codes such that*

$$\lim_{k\to\infty} \mathbb{P}[S^k \neq g_s(f_s(S^k))] = 0$$

and the message pair generated by the source encoder satisfies $P_{M_s|M_p=m_p}(m_s) = 2^{-kR'_s}$ and for all $P_{Z^n|M_sM_p}$ such that $I(M_s; Z^n|M_p) \to 0$

$$\liminf_{k\to\infty} \min_{t^k(z^n)} \mathbb{E}[d^k(S^k, t^k(Z^n))] \geq D.$$

Theorem 4. *(R'_s, R'_p, D) is achievable if*

$$R'_s > 0,$$

$$R'_s + R'_p > H(S),$$

and

$$D \leq \Delta.$$

The general idea for achievability is to consider the ϵ-typical S^k sequences and partition them into bins of equal size so that each bin contains sequences of the same type. The identity M_p of the bin is revealed to all parties, but the identity M_s of each sequence inside a bin is perfectly protected. [1] Each of such partitions is treated as a codebook. It was shown in [7] that, for the noiseless case in which Eve is given m_p instead of z^n, the distortion averaged over all such codebooks achieves the maximum distortion Δ as $k \to \infty$ and therefore there must exists one partition that achieves Δ. In order to transition from their result to our claim in Theorem 4, we only need to show

$$\min_{t^k(z^n)} \mathbb{E}[d^k(S^k, t^k(Z^n))] \geq \min_{t^k(m_p)} \mathbb{E}[d^k(S^k, t^k(M_p))].$$

Proof: First, observe that

$$\min_{t^k(\cdot)} \mathbb{E}[d^k(S^k, t^k(\cdot))] \;=\; \frac{1}{k}\sum_{i=1}^{k} \min_{t(i,\cdot)} \mathbb{E}[d(S_i, t(i,\cdot))] \tag{13}$$

Next, we claim the channel output sequence z^n does not provide Eve anything more than m_p and therefore

$$\min_{t(i,z^n)} \mathbb{E}[\frac{1}{k}\sum_{i=1}^{k} d(S_i, t(i, Z^n))] \;\geq\; \min_{t(i,m_p)} \mathbb{E}[\frac{1}{k}\sum_{i=1}^{k} d(S_i, t(i, M_p))] - 2\delta'(\epsilon) \tag{14}$$

The analysis is similar to [6], but for the sake of clarity, we present the complete proof of (14) in Appendix B.

[1] Strictly speaking, the source encoder may violate the condition (10) on $(k+1)^{|\mathcal{S}|}$ number of bins, because $(k+1)^{|\mathcal{S}|}$ is an upper bound on the number of types of sequence with length k. However, this is just a very small (polynomial in k) number of bins compared with the total number (roughly $2^{kH(S)}$) of bins. Therefore, for this small portion of "bad" bins that violates (10), we can just let the source encoder declare an error on the private message M_s and constructs the dummy M_s uniformly given the bin index m_p. This will only contribute some ϵ factor to the error probability.

Finally, combining (14) with (13) give us the desired result. ■

C. Achievability of Theorem 1

With all the elements from Section III-A and III-B, we are now ready to harvest the achievability proof of Theorem 1 using Theorems 2 and 4 by concatenating the channel encoder to the source encoder.

Proof: Fix $\nu \geq \epsilon > 0$. Fix P_S. Let ${R_s}' = 2\nu$, ${R_p}' = H(S) - \nu$ and $R' = {R_s}' + {R_p}'$. We apply the same codebook construction and encoding scheme as in Section III-B by partioning the ϵ-typical S^k sequences into $2^{kR_p{}'}$ bins and inside each bin we have $2^{kR_s{}'}$ sequences so that $\mathbb{P}[S^k \neq g_s(f_s(S^k))] \leq \epsilon$. Recall that all the sequences inside one bin are of the same type, so it is guaranteed that

$$P_{M_s|M_p=m_p}(m_s) = \frac{1}{|\mathcal{M}_s|} = \frac{1}{2^{kR_s'}}$$

for all m_p, m_s, which implies $I(M_s; M_p) = 0$.

Let R_s and R_p be the channel rates and $R_p(R_s)$ be the outer boundary of the region given in Theorem 2. Suppose $\max_{(R_s,R_p)\in\mathcal{R}} R_s > 0$, i.e. there exists W–□–X–□–YZ such that $I(W;Y) - I(W;Z) > 0$ (justified in Appendix C). $R_p(R_s)$ is continuous and non-increasing. Thus, R_p achieves the maximum at $R_s = 0$, which would be the channel capacity $\max_X I(X;Y)$ of $P_{Y|X}$ for reliable transmission. By the continuity of $R_p(R_s)$, $(R_s, R_p) = (2R\nu, R_p(0) - \delta(\nu))$ is achievable under strong secrecy, i.e. $\mathbb{P}[(M_s, M_p) \neq (\hat{M}_s, \hat{M}_p)] \leq \epsilon$ and $I(M_s; Z^n|M_p) \leq \epsilon$, where $\delta(\nu) \leq B2R\nu \to 0$ as $\nu \to 0$, and $B = \max_{R_s} R_p(R_s) = R_p(0)$.

From the above good channel code under strong secrecy we have $P_{Z^n|M_sM_p}$ such that $I(M_s; Z^n|M_p) \to 0$. Therefore, we can apply Theorem 4 to achieve

$$\liminf_{k\to\infty} \min_{t^k(z^n)} \mathbb{E}[d^k(S^k, t^k(Z^n))] = D.$$

The error probability is bounded by the sum of the error probabilities from the source coding and channel coding parts i.e. $\mathbb{P}[S^k \neq \hat{S}^k] < 2\epsilon$. Finally, we verify the total transmission rate to

complete the proof:

$$\begin{aligned} R &= \frac{k}{n} = \frac{R_s + R_p}{R'_s + R'_p} \\ &= \frac{R_p(0) + 2(B+1)R\nu}{H(S) + \nu} \\ &\geq \frac{R_p(0)}{H(S) + \nu} \\ &= \frac{\max_X I(X;Y)}{H(S) + \nu}. \end{aligned}$$

■

We next state the rate-distortion result for source-channel coding with an i.i.d. source sequence and discrete memoryless broadcast channel $P_{YZ|X}$ when **causal information** is available to Eve. The result comes from the rate matching of [6].

Theorem 5. *For an i.i.d. source sequence S^k and a memoryless broadcast channel $P_{YZ|X}$, a rate distortion pair (R, D) is achievable if*

$$\begin{aligned} R &\leq \min\left(\frac{I(V;Y)}{I(S;U)}, \frac{I(W;Y|V) - I(W;Z|V)}{H(S|U)}\right), \\ RD &\leq \alpha \cdot \Delta + (1-\alpha) \cdot \min_{t(u)} \mathbb{E}[d(S, t(U))] \end{aligned}$$

for some distribution $P_S P_{U|S} P_V P_{W|V} P_{X|W} P_{YZ|X}$, where $\alpha = \frac{[I(V;Y) - I(V;Z)]^+}{I(S;U)}$.

IV. MMF Main Results

We now return to the MMF model introduced in Section II. With the theoretical results obtained from the previous section, we have the tools needed to find the rate distortion regions for the MMF model defined in (3) and (5) under the two scenarios. In this section, we assume the channels are constant. First of all, we will give the achievable rate region under strong secrecy (therefore also under weak secrecy).

Theorem 6. *The following rate region for one private and one non-private message is achievable under strong secrecy for a complex Gaussian channel:*

$$R_s \leq \log \frac{|HKH^\dagger + \sigma_N^2 I|}{|\sigma_N^2 I|} - \log \frac{|H^e K H^{e\dagger} + \sigma_{N^e}^2 I|}{|\sigma_{N^e}^2 I|} \tag{15}$$

$$R_p \leq \log \frac{|HQH^\dagger + \sigma_N^2 I|}{|HKH^\dagger + \sigma_N^2 I|} \tag{16}$$

for some K and Q, where $0 \preceq K \preceq Q$, $K \in \mathcal{H}^{M\times M}$, Q satisfies the power constraint in (2), and H and H^e are the channel gain matrices.

Proof: According to Theorem 2 and 3,

$$R_s \leq I(W;Y|V) - I(W;Z|V) \tag{17}$$

$$R_p \leq I(V;Y) \tag{18}$$

for some V–□–W–□–X–□–YZ and $\mathbb{E}[XX^\dagger] \leq Q$, is an achievable rate pair.

We restrict the channel input X to be a circularly symmetric complex Gaussian vectors. Let $V \sim \mathcal{CN}(0, Q-K, 0)$, $B \sim \mathcal{CN}(0, K, 0)$ such that B and V are independent, and $W = X = V + B$. Therefore, $X \sim \mathcal{CN}(0, Q, 0)$ satisfies the power constraint. Similar to [3], the rate pair (R_s, R_p) satisfying inequalities (15) and (16) can be achieved. ■

An immediate corollary follows directly from the above theorem.

Corollary 1. *The following rate pairs are achievable under strong secrecy for MMF with channel gains defined in (4) and (6) and equal full power allocation $Q = I$:*

$$R_s \leq \log \frac{|\mathit{SNR} K + I|}{|\mathit{SNR}^e \Psi^e K \Psi^{e\dagger} \Phi + I|} \tag{19}$$

$$R_p \leq \log \frac{|(\mathit{SNR}+1) I|}{|\mathit{SNR} K + I|} \tag{20}$$

for some K where $0 \preceq K \preceq I$, $K \in \mathcal{H}^{M\times M}$, $\mathit{SNR} = E_0 L/\sigma_N^2$ and $\mathit{SNR}^e = E_0 L^e/\sigma_{N^e}^2$.

With the secrecy capacity region of MMF, we can evaluate its rate distortion region (R, D) under the two extreme cases, without and with causal information at Eve's decoder respectively.

For the best case scenario (no causal information), we will give a sufficient condition to force maximum distortion Δ between Alice and Eve. For the worst case scenario (with causal information), we will give an achievable rate-distortion region and look at the particular case of Hamming distortion, defined as:

$$d(s,t) = \begin{cases} 0, & s = t, \\ 1, & \text{otherwise.} \end{cases}$$

Theorem 7. *For an i.i.d source sequence S^k, if*

$$\min_{j\in\{1,\ldots,M\}} \bar{\phi}_j < \frac{SNR}{SNR^e} \tag{21}$$

where $\bar{\phi}_j$'s are the diagonal entries of Φ, then the following rate distortion pair (R, D) is achievable with ***no causal information*** *at the eavesdropper:*

$$R < \frac{M\log(SNR+1)}{H(S)} \tag{22}$$

$$D \leq \Delta. \tag{23}$$

Theorem 7 follows from Theorem 1 and Corollary 1. Note that (21) is a sufficient condition for the existence of a secure channel with strictly positive rate from Alice to Bob. An discussion on this condition is provided in Appendix D.

Theorem 8. *For an i.i.d. source sequence S^k and Hamming distortion, the following distortion rate curve $D(R)$ is in the achievable region* ***with causal information*** *at the eavesdropper:*

$$D = d(H(S)), \text{ if } R \leq \frac{R_s^*}{H(S)} \tag{24}$$

$$D = \bar{\alpha}(K)\Delta + (1-\bar{\alpha}(K))d(\frac{R_s(K)}{R}), \text{ if } \frac{R_s^*}{H(S)} < R \leq \frac{R_p^*}{H(S)} \tag{25}$$

where $d(R_s') \triangleq \min(f(R_s'), 1-\max_s P_S(s))$ and $f(R_s')$ is the linear interpolation of the points $(\log n, \frac{n-1}{n})$, $n = 1,2,3,\ldots$; $\mathcal{K} \triangleq \{K \in \mathcal{H}^{M\times M}, 0 \preceq K \preceq I\}$,

$$R_s^* = \max_{K'\in\mathcal{K}} \log \frac{|SNRK' + I|}{|SNR^e\sqrt{\Phi}\Psi^e K'\Psi^{e\dagger}\sqrt{\Phi} + I|},$$

$$R_p^* = M \log(\boldsymbol{SNR} + 1),$$

$$R_s(K) = \log \frac{|\boldsymbol{SNR}K + I|}{|\boldsymbol{SNR}^e \sqrt{\Phi}\Psi^e K \Psi^{e\dagger}\sqrt{\Phi} + I|},$$

$$\bar{\alpha}(K) = \frac{\bar{\beta}(K) - \bar{\gamma}(K)}{\bar{\beta}(K)},$$

$$\bar{\beta}(K) = \log \frac{|(\boldsymbol{SNR} + 1)I|}{|\boldsymbol{SNR}K + I|},$$

$$\bar{\gamma}(K) = \log \frac{|\boldsymbol{SNR}^e \Phi + I|}{|\boldsymbol{SNR}^e \sqrt{\Phi}\Psi^e K \Psi^{e\dagger}\sqrt{\Phi} + I|}.$$

The result given in Theorem 8 can be derived directly from Theorem 5 and Corollary 1.

V. Numerical Results

In this section, we present numerical results illustrating achievable rate distortion regions of an MMF under the two information models. Let us consider measuring the eavesdropper's distortion using Hamming distortion and a Bern(p) i.i.d. source sequence. Fig. 3 shows numerical results corresponding to Theorem 7 and Theorem 8 under equal power allocation. The channels are simulated as a $4-$mode MMF with SNR $= 20dB$, SNR$^e = 10dB$, and MDL $= 20dB$.

In each plot, the vertical line on the right is the maximum reliable transmission rate between Alice and Bob and the vertical line on the left is the maximum perfect secrecy transmission rate that can be obtained with separate source-channel coding. The horizontal line is the maximum distortion which is also the rate distortion curve from Theorem 7 with no causal information at Eve. The curve obtained from Theorem 8 shows the tradeoff between the transmission rate between Alice and Bob and the distortion forced to Eve with causal information. We see in Fig. 3(a), $p = 0.3$, that with our source-channel coding analysis, we gain a free region (from the left vertical line to the kink) for maximum distortion as if under perfect secrecy because we here made better use of the redundancy of the source. In Fig. 3(b) with $p = 0.5$, since there is no redundancy in the source, the distortion curve drops immediately after the maximum perfect secrecy rate. Note that the transmission rates are not considered beyond the right vertical

lines because they are above the maximum reliable transmission rates and Bob cannot losslesly reconstruct the source sequences.

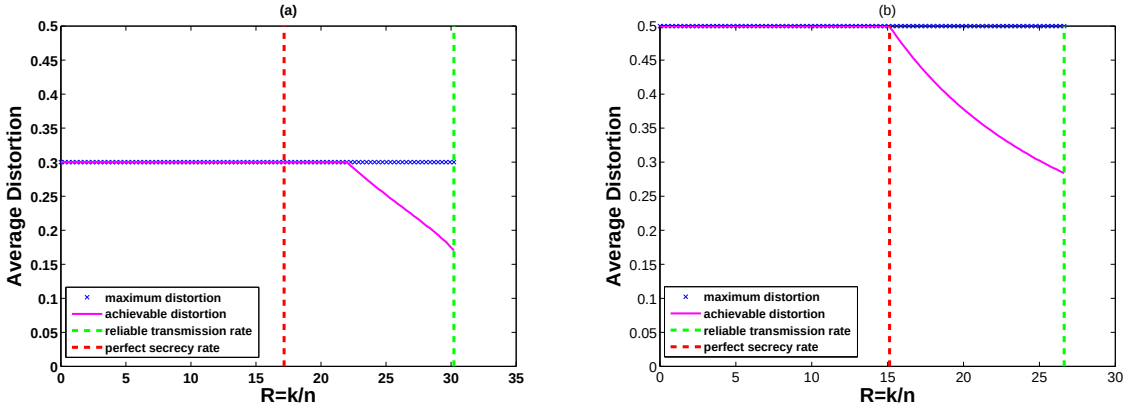

Fig. 3: Achievable distortion-rate curves. On the left is the Bern(0.3) i.i.d. source case and on the right is the Bern(0.5) i.i.d. source case. On the x-axes are the symbol/channel use source-channel coding rate and on the y-axes are the average Hamming distortions.

VI. Random Channel

So far, we have only considered the rate distortion tradeoff under deterministic channels H and H^e, i.e. the transmitter and receivers know the channel matrix before they design the codes and the channels stay constant. In the previous sections, we showed the existence of source-channel codes that guarantee a designed level of distortion inflicted on an eavesdropper under two different information assumptions. However, in MMF, the channels H and H^e vary with time and the CSI is not available at the transmitter even though it has a long coherence time. Recall from Section II, the randomness of $H = \sqrt{E_0 L}\Psi$ and $H^e = \sqrt{E_0 L^e}\sqrt{\Phi}\Psi^e$ comes from the unitary component Ψ, Ψ^e and the diagonal component Φ. The distribution of Ψ, Ψ^e, and Φ are assumed to be independent and they are i.i.d. processes for each coherence time. The random matrices Ψ and Ψ^e are uniformly distributed in $\ominus$, where $\ominus$ is the set of all $M \times M$ unitary matrices [1]. The diagonal matrix $\Phi = diag\{\bar{\phi}_1, ..., \bar{\phi}_M\}$, where $\bar{\phi}_i = M\frac{\phi_i}{\sum_{j=1}^{M}\phi_j}$. Here

$\phi_1 = \phi_{min}$ and $\phi_2 = \phi_{max}$ are fixed constants throughout the entire communication for some positive ϕ_{min} and ϕ_{max}, and $\phi_i \sim Unif[\phi_{min}, \phi_{max}]$ for $i = 3, ..., M$.

Since the channels have long coherence times, the average performance is typically measured by outage probability. We define the outage probability of rate C_{out} under power allocation strategy Q to be

$$P_{out}(Q, C_{out}) = \mathbb{P}_{\Phi\Psi^e\Psi}[R_s(Q) < C_{out}], \tag{26}$$

where $R_s(Q) \triangleq I(X;Y) - I(X;Z)$, $Q \triangleq \mathbb{E}[XX^\dagger]$. $R_s(Q)$ is the "secrecy capacity" (maximum rate for perfect secrecy) under power allocation Q of the MMF system. Note that $R_s(Q)$ is a random variable because the channels $P_{YZ|X}$ are now random. The capacity $C = \max_Q \log|I + HQH^\dagger|$ and secrecy capacity $C_s = \max_Q[\log|I+HQH^\dagger| - \log|I+H^eQH^{e\dagger}|]$ for a deterministic MIMO Gaussian broadcast channel were given in [14] and [15], respectively.

For random channels, typically, an outage occurs (i.e. $R_s(Q) < C_{out}$), if either reliable transmission to the legitimate receiver fails or perfect secrecy is violated. However, because of the unitary property of the MMF channel, the maximum reliable transmission rate under power allocation strategy Q is constant at $\log|I + \text{SNR} \cdot Q|$ which does not depend on the distribution of Ψ. Therefore, there is only one interpretation for outage, i.e. the perfect secrecy condition is violated. Under the MMF model, we have the corresponding

$$R_s(Q) = \log|I + \text{SNR} \cdot Q| - \log|I + \text{SNR}^e \cdot \Psi^e Q \Psi^{e\dagger}\Phi|.$$

Hence, (26) can be written as

$$P_{out}(Q, C_{out}) = \mathbb{P}_{\Phi\Psi^e}(\log \frac{|I + \text{SNR} \cdot Q|}{|I + \text{SNR}^e \cdot \Psi^e Q \Psi^{e\dagger}\Phi|} < C_{out}).$$

We must now determine which power allocation strategy Q gives the smallest outage probability for a given C_{out}. It has been shown quantitatively in [16] that equal full power allocation $Q = I$ minimizes the outage probability given in (26). This explains why we focus on the case $Q = I$ in earlier sections.

VII. Conclusion

In this work, we have examined the rate-distortion-based secrecy performance of an insecure MMF communication system. The sender is assumed to have an i.i.d. source sequence which the intended receiver and the eavesdropper both try to reconstruct. Two source-channel coding models with different information availability at the eavesdropper have been considered. We have shown that, when no causal source information is disclosed to the eavesdropper, under a general broadcast channel and any distortion measure, it is possible to send the source at the maximum rate that guarantees lossless reconstruction at the intended receiver while keeping the distortion at the eavesdropper as high as if it only has the source prior distribution. When the past source realization is causally disclosed to the eavesdropper, we have applied the theoretical results in [6] to the particular case of MMF channel. Numerical results for i.i.d. Bernoulli source and Hamming distortion have been provided.

It was further argued that equal full power allocation minimized outage probability under the random channel setup. However, this power allocation strategy is only supported by quantitative results from [16]. The optimality of this strategy remains an open problem. Moreover, in our model, it is required that the intended receiver reconstruct the source losslessly. In a more general setting, one can allow lossy reconstruction of the source at the intended receiver, which is an interesting problem for further research.

APPENDIX A
PROOF OF LEMMA 2

Given (m_s, m_p), suppose there exists θ_{m_p} such that

$$||P_{Z^n|M_p=m_p,M_s=m_s} - \theta_{m_p}||_{TV} \leq \epsilon_n \tag{27}$$

where $\epsilon_n = 2^{-n\beta}$ for some $\beta > 0$ Then we have the following:

$$\begin{aligned}
& ||P_{Z^n|M_p=m_p} - \theta_{m_p}||_{TV} \\
= & \sum_{z^n} \left| P_{Z^n|M_p=m_p(z^n)}(z^n) - \theta_{m_p}(z^n) \right| && (28) \\
= & \sum_{z^n} \left| \sum_{m_s} P_{M_s|M_p=m_p}(m_s) P_{Z^n|M_p=m_p,M_s=m_s}(z^n) - \sum_{m_s} P_{M_s|M_p=m_p}(m_s)\theta_{m_p}(z^n) \right| \\
= & \sum_{z^n} \left| \sum_{m_s} \frac{1}{|\mathcal{M}_s|} P_{Z^n|M_p=m_p,M_s=m_s}(z^n) - \sum_{m_s} \frac{1}{|\mathcal{M}_s|}\theta_{m_p}(z^n) \right| \\
\leq & \sum_{z^n}\sum_{m_s} \frac{1}{|\mathcal{M}_s|} \left| P_{Z^n|M_p=m_p,M_s=m_s}(z^n) - \theta_{m_p}(z^n) \right| && (29) \\
= & \sum_{m_s} \frac{1}{|\mathcal{M}_s|} \sum_{z^n} \left| P_{Z^n|M_p=m_p,M_s=m_s}(z^n) - \theta_{m_p}(z^n) \right| \\
\leq & \sum_{m_s} \frac{1}{|\mathcal{M}_s|} \epsilon_n && (30) \\
= & \epsilon_n && (31)
\end{aligned}$$

where (29) follows from triangle inequality and (30) follows from (27).

$$
\begin{aligned}
& ||P_{Z^n|M_p=m_p}P_{M_s|M_p=m_p} - P_{Z^nM_s|M_p=m_p}||_{TV} \\
= & \sum_{z^n}\sum_{m_s}\left|P_{Z^n|M_p=m_p}(z^n)P_{M_s|M_p=m_p}(m_s) - P_{Z^n|M_p=m_p,M_s=m_s}(z^n)P_{M_s|M_p=m_p}(m_s)\right| \\
= & \frac{1}{|\mathcal{M}_s|}\sum_{z^n}\sum_{m_s}\left|P_{z^n|M_p=m_p}(z^n) - P_{Z^n|M_p=m_p,M_s=m_s}(z^n)\right| \\
= & \frac{1}{|\mathcal{M}_s|}\sum_{z^n}\sum_{m_s}\left|P_{Z^n|M_p=m_p}(z^n) - \theta_{m_p}(z^n) + \theta_{m_p}(z^n) - P_{Z^n|M_p=m_p,M_s=m_s}(z^n)\right| \\
\leq & \frac{1}{|\mathcal{M}_s|}\sum_{z^n}\sum_{m_s}(\left|P_{Z^n|M_p=m_p}(z^n) - \theta_{m_p}(z^n)\right| + \left|P_{Z^n|M_p=m_p,M_s=m_s}(z^n) - \theta_{m_p}(z^n)\right|) \\
= & \frac{1}{|\mathcal{M}_s|}\sum_{m_s}(\sum_{z^n}\left|P_{Z^n|M_p=m_p}(z^n) - \theta_{m_p}(z^n)\right| + \sum_{z^n}\left|P_{Z^n|M_p=m_p,M_s=m_s}(z^n) - \theta_{m_p}(z^n)\right|) \\
\leq & \frac{1}{|\mathcal{M}_s|}\sum_{m_s}(\epsilon_n + \epsilon_n) \\
= & 2\epsilon_n
\end{aligned}
$$

By applying Lemma 1, we have

$$
\begin{aligned}
I(M_s; Z^n|M_p) &= \sum_{m_p} P_{M_p}(m_p) I(M_s; Z^n|M_p = m_p) \\
&\leq \sum_{m_p} P_{M_p}(m_p)(-2\epsilon_n \log \frac{2\epsilon_n}{|\mathcal{M}_s||\mathcal{Z}|^n}) \\
&\leq 2 \cdot 2^{-n\beta}(nR_s + n\log|\mathcal{Z}|) \qquad (32)
\end{aligned}
$$

where (32) goes to 0 as $n \to \infty$.

APPENDIX B
PROOF OF (14)

For each i, we have

$$
\begin{aligned}
I(S_i; Z^n|M_p) &\leq I(M_sS_i; Z^n|M_p) \\
&= I(M_s; Z^n|M_p) + I(S_i; Z^n|M_sM_p) \\
&\leq \epsilon \qquad (33)
\end{aligned}
$$

for large enough n. (33) follows from strong secrecy of the channel and Fano's inequality. We now define

$$P_i \triangleq P_{S_i Z^n M_p}$$

$$\bar{P}_i \triangleq P_{M_p} P_{S_i|M_p} P_{Z^n|M_p}$$

i.e. $\bar{P}_i$ is the Markov chain S_i–□–M_p–□–Z^n. By Pinsker's inequality,

$$\begin{aligned} ||P_i - \bar{P}_i||_{TV} &\leq \frac{1}{\sqrt{2}} D(P_i||\bar{P}_i)^{\frac{1}{2}} \\ &= \frac{1}{\sqrt{2}} I(S_i; Z^n|M_p)^{\frac{1}{2}} \\ &\leq \sqrt{\frac{\epsilon}{2}} \end{aligned} \tag{34}$$

$$\begin{aligned} \min_{t(i,z^n)} \mathbb{E}[d(S_i, t(i, Z^n))] &\geq \min_{t(i,z^n,m_p)} \mathbb{E}[d(S_i, t(i, Z^n, M_p))] \\ &\geq \min_{t(i,z^n,m_p)} \mathbb{E}_{\bar{P}_i}[d(S_i, t(i, Z^n, M_p))] - \delta'(\epsilon) && (35) \\ &= \min_{t(i,m_p)} \mathbb{E}_{\bar{P}_i}[d(S_i, t(i, M_p))] - \delta'(\epsilon) && (36) \\ &\geq \min_{t(i,m_p)} \mathbb{E}[d(S_i, t(i, M_p))] - 2\delta'(\epsilon) && (37) \end{aligned}$$

where (35) and (37) use the fact that P_i and $\bar{P}_i$ are close in total variation from (34); (36) uses the Markov relation S_i–□–M_p–□–Z^n of distribution $\bar{P}_i$. The technical details can be found in Lemma 2 and 3 from [6]. Averaging over k, we obtain (14).

APPENDIX C
JUSTIFICATION OF THE CONDITION $\max_{(R_s,R_p)\in\mathcal{R}} R_s > 0$

From Theorem 2 or 3, we have

$$\max_{(R_s,R_p)\in\mathcal{R}} R_s > 0$$

is equivalent to

$$I(W;Y|V) - I(W;Z|V) \;>\; 0 \tag{38}$$

for some V–□–W–□–X–□–YZ. We claim this can be simplified as

$$I(W;Y) - I(W;Z) \;\; > \;\; 0 \tag{39}$$

for some W–□–X–□–YZ.

To see $(39) \Rightarrow (38)$, we can just let $V = \emptyset$. To see $(38) \Rightarrow (39)$, observe that if there exists V–□–W–□–X–□–YZ such that (38) holds, then there has to exist at least one value v such that $I(W;Y|V=v) - I(W;Z|V=v) > 0$. We can redefine the distribution as $P_{\bar{W}\bar{X}\bar{Y}\bar{Z}} \triangleq P_{WXYZ|V=v}$. It can be verified that the Markovity $\bar{W}$–□–$\bar{X}$–□–$\bar{Y}\bar{Z}$ holds and $P_{\bar{Y}\bar{Z}|\bar{X}} = P_{YZ|X}$.

APPENDIX D
SUFFICIENT CONDITION ON THEOREM 7

From Theorem 1 and Corollary 1, we know that a sufficient condition for the eavesdropper's channel not being less noisy than the intended receiver's channel is

$$\max_{K \in \mathcal{H}^{M\times M}, 0 \preceq K \preceq I} \frac{|\text{SNR}K + I|}{|\text{SNR}^e \Psi^e K \Psi^{e\dagger} \Phi + I|} > 1. \tag{40}$$

However, (40) is computationally heavy to verify. If we restrict K to be of the form $K = \Psi^{e\dagger} \Lambda \Psi^e$ where Λ is diagonal with diagonal entries $\lambda_i \in [0,1]$, then (40) has a much simpler form:

$$\frac{\prod_{i=1}^{M}(1 + \text{SNR}\lambda_i)}{\prod_{i=1}^{M}(1 + \text{SNR}^e \lambda_i \bar{\phi}_i)} > 1. \tag{41}$$

Therefore, if there exists a $j \in \{1, ..., M\}$ such that $\bar{\phi}_j < \frac{\text{SNR}}{\text{SNR}^e}$, we can choose $\lambda_j = 1$ and $\lambda_i = 0$ for $i \neq j$ to satisfy (41).

ACKNOWLEDGMENT

The authors would like to thank Dr. Kyle Guan and Dr. Peter Winzer from Bell Labs, Alcatel Lucent, for fruitful discussions and great support on this project.

REFERENCES

[1] P. J. Winzer and G. J. Foschini, "MIMO capacities and outage probabilities in spatially multiplexed optical transport systems," Optics Express, Vol. 19, pp. 16680-16696, 2011.

[2] K. Guan, P. J. Winzer, and E. Soljanin, "Information-theoretic security in space-division multiplexed fiber optic networks," Proc. European Conference on Optical Communications, 2012.

[3] T. Liu and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," IEEE Trans. Inf. Theory, Vol 56, pp. 5477-5487, 2010.

[4] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," IEEE Trans. Inf. Theory, Vol. 43, pp. 827-835, 1997.

[5] P. Cuff, "A framework for partial secrecy," Global Communications Conference, 2010.

[6] C. Schieler, E. C. Song, P. Cuff, and H. V. Poor., "Source-channel secrecy with causal disclosure," Proc. 50th Annual Allerton Conf. Commun. Contr. Comput., 2012.

[7] C. Schieler and P. Cuff, "Secrecy is cheap if the adversary must reconstruct," Proc. International Symposium on Information Theory, 2012.

[8] I. Csiszár and J. Körner, "Broadcast channels with confidential messages", IEEE Trans. Inf. Theory, Vol. 24, pp.339-348, 1978.

[9] A. D. Wyner, "The wire-tap channel," Bell. Syst. Tech. J. vol. 54, no. 8, pp. 1355-1387, 1975.

[10] U. Maurer and S. Wolf, "Information-theoretic key agreement: from weak to strong secrecy for free," Lecture Notes in Computer Science, Vol. 1807/2000, pp. 351-368, 2000.

[11] J. Barros and M. Bloch "Strong secrecy for wireless channels," Lecture Notes in Computer Science, Vol. 5155/2008, pp. 43-53, 2008.

[12] R. F. Wyrembelski and H. Boche "Strong secrecy in compound broadcast channels with confidential messages," Proc. International Symposium on Information Theory, 2012.

[13] I. Csiszár and J. Körner, Information Theory: Coding Theorems for Discrete Memoryless Systems (2nd ed), Cambridge University Press, pp. 19-20, 2011.

[14] E. Teletar, "Capacity of multi-antenna Gaussian channels," European Transactions on Telecommunications, Vol. 10, pp. 585-595, 1999.

[15] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Trans. Inf. Theory, Vol. 57, pp. 4961-4972, 2011.

[16] K. C. Guan, E. C. Song, E. Soljanin, P. J. Winzer, and A. M. Tulino, "Physical layer security in space-division multiplexed fiber optic communications," Proc. Asilomar Conference on Signals, Systems, and Computers, 2012.